Claims:

1. A method of authenticating candidate members wishing to participate in an IP multicast via a communication network, where data sent as part of the multicast is to be secured using a key revocation based scheme requiring that each candidate member submit a public key to a group controller, the method comprising:

at the group controller, verifying that the public key received from each candidate member is owned by that member and that it is associated with the IP address of that candidate member by inspecting an interfaceID part of the IP address.

2. A method according to claim 1, wherein said key revocation based scheme is a Logical Key Hierarchy based scheme.

3. A method according to claim 1 or 2, wherein each candidate member generates an interfaceID part of its own IPv6 address by taking a cryptographic hash over its own public key and one or more other parameters, and a candidate member sends a joining request to the group controller which contains: the member's IP address including the generated interface ID; its own public key; and a signature over the entire message generated using the member's private key.

4. A method according to claim 3, wherein upon receipt of the message, the group controller: a) uses the received public key to confirm that the signature is valid, thus proving that the candidate member does indeed own the public-private key pair to which the received public key belongs and b) applies the same cryptographic hash (as used by the candidate member) to the public key and the other parameter(s) and compares the result to the interfaceID part of the member's IP address, thus verifying that the source IP address is owned by the candidate member.

5. A method according to claim 2 or to claim 3 or 4 when appended to claim 2, wherein, after group controller has received the public key from a given member and has verified that the public key is associated with the IP address of the sender, the group controller sends a unique Key Encryption Key to the member, encrypted with that member's public key, and the group controller also sends a Traffic Encryption Key and a LKH key set to the member, encrypted with the Key Encryption Key.

6. A method according to any one of the preceding claims, wherein said IP multicast comprises: a one-way multicast where a single node multicasts a stream of data to several other nodes; a group multicast where group members multicast data to all other members of the group; or a tele- or videoconference or a multimedia conference.

7. A method of authorising a user to participate in a secure IP multicast or broadcast and in which security keys are distributed to group members using a key revocation based mechanism, the method comprising:

delivering a certificate to the user, the certificate verifying that a public-private key pair identified in the certificate can be validly used by the user to access said secure multicast/broadcast;

subsequently verifying at a control node that the certificate is owned by the user using a proof-of-possession procedure; and

assuming that verification is obtained, using said public key to send a Key Encryption Key to the user.

8. A method according to claim 7, wherein said key revocation based scheme is a Logical Key Hierarchy based scheme.

9. A method according to claim 8, wherein said step of verifying at a control node that the certificate is owned by the user, is carried out after the control node receives a request from the user to join said secure multicast or broadcast.

10. A method according to claim 7, 8, or 9, wherein said proof-of-possession procedure involves the control node sending a random number (nonce) to the user in plain text, and the user sends a response to the control node containing a signature generated by applying the private key to the random number, and using, wherein the control node is in possession of the user's certificate and can check whether or not the message is correctly signed with the user's private key.

11. A method according to any one of claims 7 to 10, wherein the user to be authorised has a subscription to a first, home communication network and wishes to participate in a multicast or broadcast service via a second, foreign network in which the user is roaming, the method comprising:

the visited network contacting the user's home network, upon receipt of an initial registration request from said user, to authorise the user;

following authorisation by the home network, generating a certificate relating to said service and comprising generating a public-private key pair, either at the user equipment or within one of the networks, and signing the certificate; and

sending the certificate to the user.

12. A method according to claim 11, wherein an AKA procedure is used to authorise the user.

13. A group controller comprising memory and processing means for implementing the method of any one of the preceding claims.

14. A mobile terminal comprising memory and processing means for implementing the method of any one of the preceding claims.